

Document made available under the Patent Cooperation Treaty (PCT)

International application number: PCT/JP05/004873

International filing date: 14 March 2005 (14.03.2005)

Document type: Certified copy of priority document

Document details: Country/Office: JP
Number: 2004-073086
Filing date: 15 March 2004 (15.03.2004)

Date of receipt at the International Bureau: 28 April 2005 (28.04.2005)

Remark: Priority document submitted or transmitted to the International Bureau in compliance with Rule 17.1(a) or (b)



World Intellectual Property Organization (WIPO) - Geneva, Switzerland
Organisation Mondiale de la Propriété Intellectuelle (OMPI) - Genève, Suisse

日 本 国 特 許 庁
JAPAN PATENT OFFICE

14. 3. 2005

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出 願 年 月 日
Date of Application: 2 0 0 4 年 3 月 1 5 日

出 願 番 号
Application Number: 特 願 2 0 0 4 - 0 7 3 0 8 6

パリ条約による外国への出願
に用いる優先権の主張の基礎
となる出願の国コードと出願
番号

The country code and number
of your priority application,
to be used for filing abroad
under the Paris Convention, is

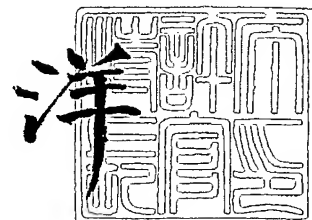
J P 2 0 0 4 - 0 7 3 0 8 6

出 願 人
Applicant(s): 松下電器産業株式会社

2 0 0 5 年 4 月 1 5 日

特許庁長官
Commissioner,
Japan Patent Office

小 川



【書類名】 特許願
【整理番号】 2048160109
【提出日】 平成16年 3月15日
【あて先】 特許庁長官 殿
【国際特許分類】 G09C
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 中野 稔久
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 石原 秀志
【発明者】
 【住所又は居所】 大阪府門真市大字門真 1 0 0 6 番地 松下電器産業株式会社内
 【氏名】 館林 誠
【特許出願人】
 【識別番号】 000005821
 【氏名又は名称】 松下電器産業株式会社
【代理人】
 【識別番号】 100090446
 【弁理士】
 【氏名又は名称】 中島 司朗
【手数料の表示】
 【予納台帳番号】 014823
 【納付金額】 21,000円
【提出物件の目録】
 【物件名】 特許請求の範囲 1
 【物件名】 明細書 1
 【物件名】 図面 1
 【物件名】 要約書 1
 【包括委任状番号】 9003742

【書類名】 特許請求の範囲**【請求項 1】**

データ、並びに許可情報を受信する、あるいは前記データを暗号化する暗号化装置の集積回路であって、

前記集積回路は、前記データ、並びに前記許可情報を受信する受信部と、前記許可情報に自身の認証情報を生成して付加する認証情報生成部と、生成した認証情報付き許可情報を送信する送信部を備えることを特徴とする集積回路。

【請求項 2】

前記集積回路であって、

前記集積回路は、前記認証情報を生成するための固有情報を保持する格納部を備え、

前記固有情報に基づいて前記認証情報付き許可情報を生成することを特徴とする請求項 1 記載の集積回路。

【請求項 3】

前記集積回路であって、

前記集積回路の前記認証情報生成部は、前記固有情報に基づき、認証情報として、秘密鍵暗号を利用して認証子データを生成することを特徴とする請求項 2 記載の集積回路。

【請求項 4】

前記集積回路であって、

前記集積回路の前記認証情報生成部は、前記固有情報に基づき、認証子情報として、公開鍵暗号を利用して署名データを生成することを特徴とする請求項 2 記載の集積回路。

【請求項 5】

前記集積回路であって、

前記集積回路の前記認証情報生成部は、前記認証情報を生成する際、前記データの暗号化を許可する他の暗号化装置の識別情報を追加して認証情報を生成することを特徴とする請求項 1 記載の集積回路。

【請求項 6】

前記集積回路であって、

前記集積回路の前記認証情報生成部が生成する前記認証情報は、複数の暗号化装置の識別情報を含むことを特徴とする請求項 5 記載の集積回路。

【請求項 7】

前記集積回路であって、

前記集積回路は、前記配布装置から受信部を介して受信した前記データ、並びに前記認証情報生成部で生成した認証情報付き許可情報を、前記送信部を介して、他の暗号化装置へ送信し、

前記他の暗号化装置は、前記データ、並びに前記認証情報付き許可情報を受信部を介して受信して、前記受信した前記認証情報付き許可情報を前記鍵配布装置へ前記送信部を介して送信することを特徴とする請求項 1 記載の集積回路。

【請求項 8】

暗号化装置に鍵データを供給する鍵配布装置の集積回路であって、

前記集積回路は、送信された認証情報付き許可情報を受信する受信部と、前記受信した認証情報付き許可情報を検証する検証部と、検証結果に基づいて鍵データを前記暗号化装置へ送信する送信部を備えることを特徴とする集積回路。

【請求項 9】

前記集積回路であって、

前記許可情報は、前記配布装置による署名データ、並びに暗号化装置を特定する識別情報を含み、

前記集積回路の前記検証部は、前記認証情報の検証に加え、前記署名データの検証を行うことを特徴とする請求項 8 記載の集積回路。

【請求項 10】

前記集積回路であって、

前記集積回路の前記検証部が検証する前記許可情報は、複数の暗号化装置の識別情報を含むことを特徴とする請求項 9 記載の集積回路。

【請求項 1 1】

前記集積回路であって、

前記集積回路は、前記受信した許可情報が、認証情報付きであるか否かを判定する判定部を備え、

前記判定部が認証情報なしを判定した場合、前記検証部は、前記許可情報の署名データのみを検証して、前記判定部が認証情報付きと判定した場合は、前記検証部は、前記許可情報の署名データに加え、認証情報を検証することを特徴とする請求項 9 記載の集積回路。

【請求項 1 2】

前記集積回路であって、

前記集積回路は、前記認証情報付き許可情報を前記受信部を介して受信して、前記検証部で検証した結果に基づいて、前記暗号化装置が個別に保持する固有鍵を用いて前記鍵データを暗号化して、前記送信部を介して前記暗号化した鍵データを送信することを特徴とする請求項 8 記載の集積回路。

【請求項 1 3】

前記集積回路であって、

前記集積回路が前記検証部で検証する前記認証情報付き許可情報は、複数の暗号化装置の識別情報、並びに複数の認証情報を含むことを特徴とする請求項 8 記載の集積回路。

【請求項 1 4】

前記集積回路であって、

前記集積回路の前記判定部は、許可情報のデータサイズに基づいて、認証情報が追加されているか否かを判定し、さらに、複数の認証情報が追加されている場合、同じくデータサイズに基づいて、前記認証情報の数を判定することを特徴とする請求項 9 記載の集積回路。

【請求項 1 5】

暗号化されたデータ、並びに許可情報を受信する、あるいは前記暗号化されたデータを復号する復号装置の集積回路であって、

前記集積回路は、前記暗号化されたデータ、並びに前記許可情報を受信する受信部と、前記許可情報に自身の認証情報を生成して付加する認証情報生成部と、生成した認証情報付き許可情報を送信する送信部を備えることを特徴とする集積回路。

【書類名】 明細書

【発明の名称】 著作権保護のための集積回路

【技術分野】

【0001】

本発明は、コンテンツデータの不正利用防止を目的としたデータ配布装置、データ暗号化装置、及び鍵配布装置を含む著作権保護システムに関し、特に、コンテンツデータの暗号化処理を実行する装置の選択を柔軟に行うことが可能となる技術に関する。

【背景技術】

【0002】

近年、デジタルコンテンツデータ（以下、コンテンツデータ）は複製が容易であるため、インターネットやその他の媒体を介した海賊行為、並びに複製コンテンツデータの再配信などの不正行為に対する懸念が高まっており、これら不正行為に対抗（コンテンツデータを保護）するための技術開発が進められている。

そのようなコンテンツデータを保護する技術の1つとして、特定の装置に対しては、コンテンツデータの暗号化処理、あるいは復号処理に必要な鍵データを供給せず、それ以外の装置に対してのみ、鍵データを供給する（暗号化処理、あるいは復号処理を許可する）ことが可能となる技術が特許文献1に開示されている。

【0003】

一方で、不正装置によるコンテンツデータの暗号化処理、あるいは復号処理を防止するために、コンテンツデータの保有者が、処理を許可する装置に対してのみ、コンテンツデータの暗号化、あるいは復号に必要な鍵が与えられる許可証を配布して、その許可証に基づいて鍵データが配布される方式も存在する。

【特許文献1】 特開2002-281013号公報

【非特許文献1】 「現代暗号理論」、池野信一、小山謙二、電子通信学会

【非特許文献2】 「暗号理論入門」、岡本栄司、共立出版株式会社

【発明の開示】

【発明が解決しようとする課題】

【0004】

しかし、前記方式では、許可証を受け取った装置だけが暗号化処理、あるいは復号処理を実行することが可能なため、実際の処理の実行を、正規に他の装置に対して依頼（委託）することが不可となってしまうシステムの柔軟性が損なわれることにつながる。

本発明は、前記課題を解決するものであって、不正装置による暗号化処理、あるいは復号処理を防止しながら、正規に処理を委託することを可能にするデータ配布装置、データ暗号化装置、鍵配布装置を含む著作権保護システムの提供を目的とする。

【課題を解決するための手段】

【0005】

本発明は、データ、並びに許可情報を受信する、あるいは前記データを暗号化する暗号化装置の集積回路であって、前記集積回路は、前記データ、並びに前記許可情報を受信する受信部と、前記許可情報に自身の認証情報を生成して付加する認証情報生成部と、生成した認証情報付き許可情報を送信する送信部を備えることを特徴とする。

また、本発明は、前記集積回路であって、前記集積回路は、前記認証情報を生成するための固有情報を保持する格納部を備え、前記固有情報に基づいて前記認証情報付き許可情報を生成することを特徴とする。

【0006】

また、本発明は、前記集積回路であって、前記集積回路の前記認証情報生成部は、前記固有情報に基づき、認証情報として、秘密鍵暗号を利用して認証子データを生成することを特徴とする。

また、本発明は、前記集積回路であって、前記集積回路の前記認証情報生成部は、前記固有情報に基づき、認証子情報として、公開鍵暗号を利用して署名データを生成することを特徴とする。

【0007】

また、本発明は、前記集積回路であって、前記集積回路の前記認証情報生成部は、前記認証情報を生成する際、前記データの暗号化を許可する他の暗号化装置の識別情報を追加して認証情報を生成することを特徴とする。

また、本発明は、前記集積回路であって、前記の集積回路の前記認証情報生成部が生成する前記認証情報は、複数の暗号化装置の識別情報を含むことを特徴とする。

【0008】

また、本発明は、前記集積回路であって、前記集積回路は、前記配布装置から受信部を介して受信した前記データ、並びに前記認証情報生成部で生成した認証情報付き許可情報を、前記送信部を介して、他の暗号化装置へ送信し、前記他の暗号化装置は、前記データ、並びに前記認証情報付き許可情報を受信部を介して受信して、前記受信した前記認証情報付き許可情報を前記鍵配布装置へ前記送信部を介して送信することを特徴とする。

【0009】

また、本発明は、暗号化装置に鍵データを供給する鍵配布装置の集積回路であって、前記集積回路は、送信された認証情報付き許可情報を受信する受信部と、前記受信した認証情報付き許可情報を検証する検証部と、検証結果に基づいて鍵データを前記暗号化装置へ送信する送信部を備えることを特徴とする。

また、本発明は、前記集積回路であって、前記許可情報は、前記配布装置による署名データ、並びに暗号化装置を特定する識別情報を含み、前記集積回路の前記検証部は、前記認証情報の検証に加え、前記署名データの検証を行うことを特徴とする。

【0010】

また、本発明は、前記集積回路であって、前記集積回路の前記検証部が検証する前記許可情報は、複数の暗号化装置の識別情報を含むことを特徴とする。

また、本発明は、前記集積回路であって、前記集積回路は、前記受信した許可情報が、認証情報付きであるか否かを判定する判定部を備え、前記判定部が認証情報なしを判定した場合、前記検証部は、前記許可情報の署名データのみを検証して、前記判定部が認証情報付きと判定した場合は、前記検証部は、前記許可情報の署名データに加え、認証情報を検証することを特徴とする。

【0011】

また、本発明は、前記集積回路であって、前記集積回路は、前記認証情報付き許可情報を前記受信部を介して受信して、前記検証部で検証した結果に基づいて、前記暗号化装置が個別に保持する固有鍵を用いて前記鍵データを暗号化して、前記送信部を介して前記暗号化した鍵データを送信することを特徴とする。

また、本発明は、前記集積回路であって、前記集積回路が前記検証部で検証する前記認証情報付き許可情報は、複数の暗号化装置の識別情報、並びに複数の認証情報を含むことを特徴とする。

【0012】

また、本発明は、前記集積回路であって、前記集積回路の前記判定部は、許可情報のデータサイズに基づいて、認証情報が追加されているか否かを判定し、さらに、複数の認証情報が追加されている場合、同じくデータサイズに基づいて、前記認証情報の数を判定することを特徴とする。

また、本発明は、暗号化されたデータ、並びに許可情報を受信する、あるいは前記暗号化されたデータを復号する復号装置の集積回路であって、前記集積回路は、前記暗号化されたデータ、並びに前記許可情報を受信する受信部と、前記許可情報に自身の認証情報を生成して付加する認証情報生成部と、生成した認証情報付き許可情報を送信する送信部を備えることを特徴とする。

【発明の効果】

【0013】

本発明によれば、当該データ暗号化装置だけが個別に保持する固有鍵に基づいて許可証を更新することにより、他の装置に対して、正規に処理を委託することが可能となり、シ

システムの柔軟性向上につながる。

【発明を実施するための最良の形態】

【0014】

以下、本発明の実施の形態について、図面を参照しながら説明する。図1は、本発明に係る著作権保護システムの全体構成を示すブロック図である。このシステムは、コンテンツデータを供給するデータ配布装置101と、前記コンテンツデータを獲得して暗号化を実行するデータ暗号化装置102、及び103と、前記コンテンツデータを暗号化するための鍵を配布する鍵配布装置104からなる。

【0015】

データ配布装置101は、コンテンツデータをデータ暗号化装置102に供給する場合、データの暗号化処理の実行を許可する許可証を、前記コンテンツデータと共に前記データ暗号化装置102に供給する。暗号化データ装置102は、前記受信した許可証を鍵配布装置104に送信し、その後、鍵配布装置104から、前記コンテンツデータを暗号化するための鍵データを暗号化された状態で受信する。

【0016】

一方で、データ暗号化装置102が、暗号化処理の実行をデータ暗号化装置103へ委託する場合、データ暗号化装置102は、データ暗号化装置102によって更新された許可証と、コンテンツデータをデータ暗号化装置103へ送信する。暗号化データ装置103は、前記受信した更新済み許可証を鍵配布装置104に送信し、その後、鍵配布装置104から、前記コンテンツデータを暗号化するための鍵データを暗号化された状態で受信する。なお、実際の暗号化アルゴリズムは、公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。その一例としては、非特許文献1、あるいは非特許文献2に、DES暗号が開示されている。

【0017】

図2は、本発明の実施の形態における、データ暗号化装置102、並びに103の機能を示す機能ブロック図である。

データ暗号化装置102、並びに103は、外部からのデータを受信する受信部201と、受信部201で受信した許可証、あるいは更新済み許可証に基づいて、鍵配布装置に対して鍵データを要求する鍵要求部202と、データ暗号化装置102、並びに103が固有に保持する固有鍵を格納する固有鍵格納部203と、前記固有鍵に基づいて認証子を生成する認証子生成部204と、鍵配布装置104から受信した暗号化された鍵データを前記固有鍵で復号する復号部205と、前記復号部で復号して得た鍵を用いてコンテンツデータを暗号化する暗号化部206と、各データ、あるいは要求を外部に送信する送信部207を備える。

【0018】

データ暗号化装置102、並びに103は、外部から受信したコンテンツデータを自身で暗号化を実行する場合には、認証子生成部204における認証子の生成は行わず、鍵要求部202を介して、コンテンツデータを暗号化するための鍵データを要求する。図3に、データ配布装置101から配布される許可証の一例を示す。許可証は、自身の発行日を示す領域と、コンテンツデータの暗号化を許可するデータ暗号化装置のIDを示す領域と、それらに対する、データ配布装置により生成された署名が付与されている。図3の例では、発行日は2003年11月4日、暗号化の実行を許可されているデータ暗号化装置は、0x000001をIDとして持つデータ暗号化装置（データ暗号化装置102）であることが示されている。データ暗号化装置102は、自身がコンテンツデータの暗号化処理の実行を許可されている場合、前記許可証を鍵配布装置104に送信して、前記コンテンツデータを暗号化するための鍵を鍵配布装置104から受信する。

【0019】

一方で、自身では暗号化を実行せず、他のデータ暗号化装置に対して暗号化処理を委託する場合には、鍵要求部202を介した鍵の要求は実行せず、認証子生成部204において前記許可証に対して認証子を付与して前記許可証を更新する。図4に、データ暗号化装

置102が更新した更新済み許可証の一例を示す。更新済み許可証は、図3に示すデータ配布装置101により発行される許可証に加えて、委託先のデータ暗号化装置のIDを示す領域と、追加したIDを示す領域を含む全ての領域に対する、委託元のデータ暗号化装置により生成された認証子が付与されている。図3の例では、暗号化処理実施の委託先は、0x000002をIDとして持つデータ暗号化装置（データ暗号化装置103）であることが示されている。前記更新済み許可証を受信してデータ暗号化装置103は、前記更新済み許可証を鍵配布装置104に送信して、前記コンテンツデータを暗号化するための鍵を鍵配布装置104から受信する。なお、実際の認証子（Message Authentication Code: MAC）生成アルゴリズムや、署名生成/検証アルゴリズムは、非特許文献1、あるいは非特許文献2に記載されている公知の任意の技術で実現可能なため、その詳細についてはここでは言及しない。

【0020】

なお、受信部201、鍵要求部202、固有鍵格納部203、認証子生成部204、復号部205、暗号化部206、送信部207等の各機能ブロックは典型的には集積回路であるLSIとして実現される。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと呼称されることもある。

【0021】

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA（Field Programmable Gate Array）や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

【0022】

図5は、本発明の実施の形態における、鍵配布装置104の機能を示す機能ブロック図である。

鍵配布装置104は、外部からのデータを受信する受信部501と、受信部501で受信した許可証、あるいは更新済み許可証に付与されている署名の正当性を検証するための検証鍵を格納する検証鍵格納部502と、前記検証鍵を用いて前記署名の正当性を検証する署名検証部503と、データ暗号化装置が個別に保持する固有鍵を格納するデータ暗号化装置固有鍵格納部504と、前記固有鍵を用いて、前記更新済み許可証に付与されている認証子の正当性を検証するための認証子検証部505と、前記署名検証部503、並びに前記認証子検証部505の検証結果に基づいて、コンテンツデータを暗号化するための鍵データを生成するか否かを判定する鍵生成判定部506と、鍵生成判定部506において、鍵を生成すると判定した場合に、前記コンテンツデータを暗号化するための鍵データを生成する鍵生成部507と、鍵生成部507が生成した鍵データを、配布するデータ暗号化装置が個別に保持する固有鍵で暗号化する暗号化部508と、前記暗号化した鍵データを外部に送信する送信部509を備える。

【0023】

鍵配布装置104は、受信部501を介して受信した許可証が更新されておらず、データ暗号化装置による認証子が付与されていない場合は、前記許可証に付与されるデータ配布装置による署名を検証して、その検証により正当性が確認されれば、コンテンツデータを暗号化するための鍵データを生成して、許可証に記載されたデータ暗号化装置が個別に保持する固有鍵を用いて、前記生成した鍵データを暗号化して配布する。

【0024】

一方で、受信部501を介して受信して許可証が更新されており認証子が付与されている場合は、まず、更新済み許可証に付与されているデータ配布装置101による署名を検

証して、その検証により正当性が確認されれば、引き続き前記認証子への検証へと移る。このとき、認証子の検証には、元々の許可証により許可されているデータ暗号化装置が個別に保持する固有鍵を用いて検証を行い、その検証により正当性が確認されれば、コンテンツデータを暗号化するための鍵データを生成して、更新済み許可証に記載された委託先であるデータ暗号化装置が個別に保持する固有鍵で暗号化する。

【0025】

また、鍵配布装置104は、許可証が更新されているか否かを、例えば、その受信してデータのサイズから判断することが可能である。例えば、図3に示す許可証の一例において、発行日を示す領域が2バイト、許可されたデータ暗号化装置のIDを示す領域が2バイト、署名を示す領域が40バイトであった場合、受信して許可証が44バイトであれば更新されていない、44バイト以上であれば更新されている、と判断することが可能である。さらに、図4に示す更新済み許可証の一例において、委託先のデータ暗号化装置のIDを示す領域が2バイト、認証子を示す領域が16バイトであった場合、例えば、受信した許可証が62バイトであれば1度だけ更新されている、また、80バイトであれば2度更新されていると判断することが可能である。また、このように複数回の更新が行われている場合は、その都度、データ暗号化装置が個別に保持する固有鍵を選択し直して認証子の検証を行い、最後に示されたIDを持つデータ暗号化装置が個別に保持する固有鍵を用いて鍵データを暗号化して送信する。

【0026】

なお、受信部501、検証鍵格納部502、署名検証部503、データ暗号化装置固有鍵格納部504、認証子検証部505、鍵生成判定部506、鍵生成部507、暗号化部508、送信部509等の各機能ブロックは典型的には集積回路であるLSIとして実現される。これらは個別に1チップ化されても良いし、一部又は全てを含むように1チップ化されても良い。

【0027】

ここでは、LSIとしたが、集積度の違いにより、IC、システムLSI、スーパーLSI、ウルトラLSIと称されることもある。

また、集積回路化の手法はLSIに限るものではなく、専用回路又は汎用プロセッサで実現してもよい。LSI製造後に、プログラムすることが可能なFPGA(Field Programmable Gate Array)や、LSI内部の回路セルの接続や設定を再構成可能なりコンフィギュラブル・プロセッサを利用しても良い。

【0028】

さらには、半導体技術の進歩又は派生する別技術によりLSIに置き換わる集積回路化の技術が登場すれば、当然、その技術を用いて機能ブロックの集積化を行ってもよい。バイオ技術の適応等が可能性としてありえる。

次に、図6、及び図7を用いて、データ配布装置101がデータ暗号化装置102に配布、並びに暗号化の実行を許可しコンテンツデータを、データ暗号化装置102がデータ暗号化装置103にその実行を委託する場合の動作について説明する。

【0029】

S601:データ配布装置101は、コンテンツデータ、並びに自身の署名を付与して暗号化処理を実行するデータ暗号化装置102を指定する許可証を、データ暗号化装置102に対して送信する。

S602:データ暗号化装置102は、S601において送信されたコンテンツデータ、並びに許可証を受信する。

【0030】

S603:データ暗号化装置102は、暗号化処理を委託するデータ暗号化装置103のIDをS602で受信した許可証に対して追加して、追加したIDを含む許可証に対して、自身が個別に保持する固有鍵を用いて認証子を生成して付与する。

S604:データ暗号化装置102は、S602において受信したコンテンツデータと、S603で委託先のID、並びに認証子を付与して更新した許可証(更新済み許可証)

を、委託先のデータ暗号化装置 103 に対して送信する。

【0031】

S605: データ暗号化装置 103 は、S604 において送信されたコンテンツデータ、並びに更新済み許可証を受信する。

S606: データ暗号化装置 103 は、S605 において受信した更新済み許可証を鍵配布装置 104 に送信するとともに、コンテンツデータを暗号化するとき用いる鍵データを要求する。

【0032】

S607: 鍵配布装置 104 は、S606 において送信された更新済み許可証を受信する。

S701: 鍵配布装置 104 は、S607 において受信した更新済み許可証に付与されたデータ配布装置 101 による署名の正当性を検証する。さらに、データ暗号化装置 102 による認証子の正当性も検証する。

【0033】

S702: S701 の検証結果が OK の場合は S703 の処理へ進み、NG の場合は処理を終了する。

S703: 鍵配布装置 104 は、コンテンツデータを暗号化するための鍵データを生成して、データ暗号化装置が個別に保持する固有鍵を用いて、前記生成した鍵データを暗号化してデータ暗号化装置 103 へ送信する。

【0034】

S704: データ暗号化装置 103 は、S703 において送信された暗号化鍵データを受信して、自身が保持する固有鍵を用いて、受信した暗号化鍵データを復号する。さらに、復号して得た鍵データを用いて、コンテンツデータの暗号化を実行する。

(その他の変形例)

(1) 本発明の実施の形態では、データ暗号化装置が暗号化処理を委託する際の許可証の更新として、固有鍵による認証子を生成する構成としたが、本発明はその構成に限定されるものではない。例えば、データ暗号化装置が署名を生成して、鍵配布装置が認証子の代わりに前記署名を検証する構成であってもよい。その場合、鍵配布装置は前記署名を検証するための検証鍵を保持する。

【0035】

(2) 本発明の実施の形態では、データ配布装置は、許可証に対して署名を付与する構成としたが、本発明はその構成に限定されるものではない。例えば、データ配布装置が固有鍵を保持して、前記固有鍵に基づいて認証子を生成する構成であってもよい。この場合、鍵配布装置はデータ配布装置の固有鍵を保持して、署名を検証する代わりに前記認証子を検証する構成であってもよい。

【0036】

(3) 本発明の実施の形態において、データ暗号化装置は、それぞれ個別の固有鍵を保持する構成としたが、本発明はその構成に限定されるものではない。例えば、あるデータ暗号化装置の集合が、共通のグループ鍵を保持して、前記グループ鍵に基づいて認証子を生成する構成であってもよい。

(4) 本発明の実施の形態において、データ配布装置により暗号化処理を許可されるデータ暗号化装置、並びにデータ暗号化装置が委託する他のデータ暗号化装置は、許可証、並びに更新済み許可証に対して 1 つだけ記載する構成としたが、本発明はその構成に限定されるものではない。例えば、複数のデータ暗号化装置、あるいは複数の委託先が記載される構成であってもよい。

【0037】

(5) 本発明の実施の形態においては、コンテンツを暗号化するデータ暗号化装置だけが存在するシステムとしたが、本発明はその構成に限定されるものではない。例えば、データ配布装置からは、暗号化されたコンテンツデータが配布され、データ復号装置が、前記暗号化コンテンツデータを復号する構成であってもよい。その際の復号に必要な鍵の入

手方法、並びに復号処理の委託方法については実施の形態に示した方法と同様の方法により実現することが可能である。

【産業上の利用可能性】

【0038】

本発明にかかる著作権保護システムは、コンテンツデータの暗号化処理を実行するデータ暗号化装置を柔軟に選択できるため、コンテンツデータの暗号化処理を正規に他へ委託することが可能となり、委託の際には、当該データ暗号化装置だけが保持する固有鍵を用いて認証子を生成することで、不正行為（不正なデータの横流し）などを防止できる著作権保護システムの実現において有用である。

【図面の簡単な説明】

【0039】

【図1】 本発明に係る著作権保護システムの全体構成を示すブロック図

【図2】 本発明の実施の形態におけるデータ暗号化装置の機能ブロック図

【図3】 本発明の実施の形態における許可証のデータ構造を示す図

【図4】 本発明の実施の形態における更新済み許可証のデータ構造を示す図

【図5】 本発明の実施の形態における鍵配布装置の機能ブロック図

【図6】 本発明の実施の形態における暗号化処理を委託する際の動作フロー

【図7】 本発明の実施の形態における暗号化処理を委託する際の動作フロー

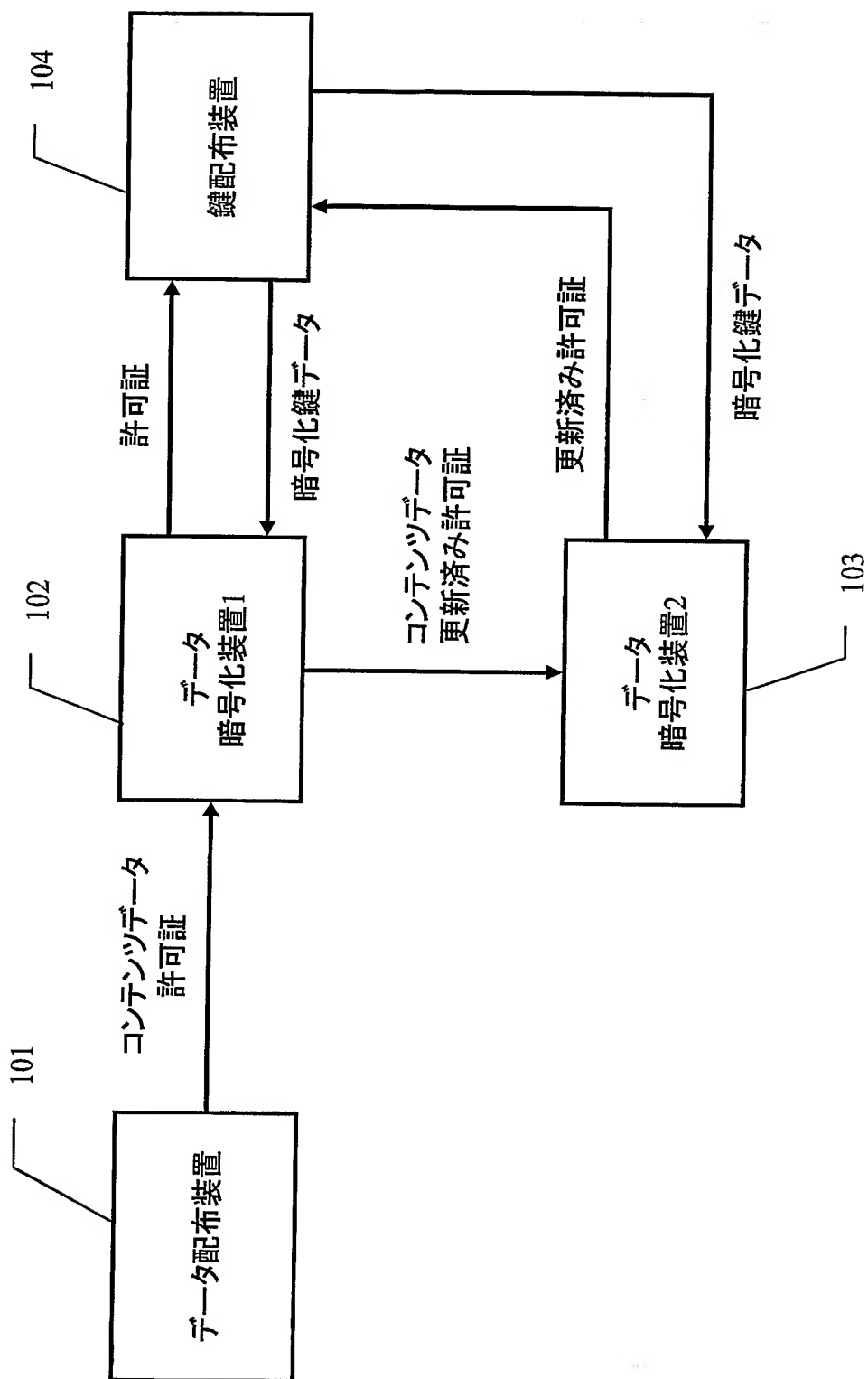
【符号の説明】

【0040】

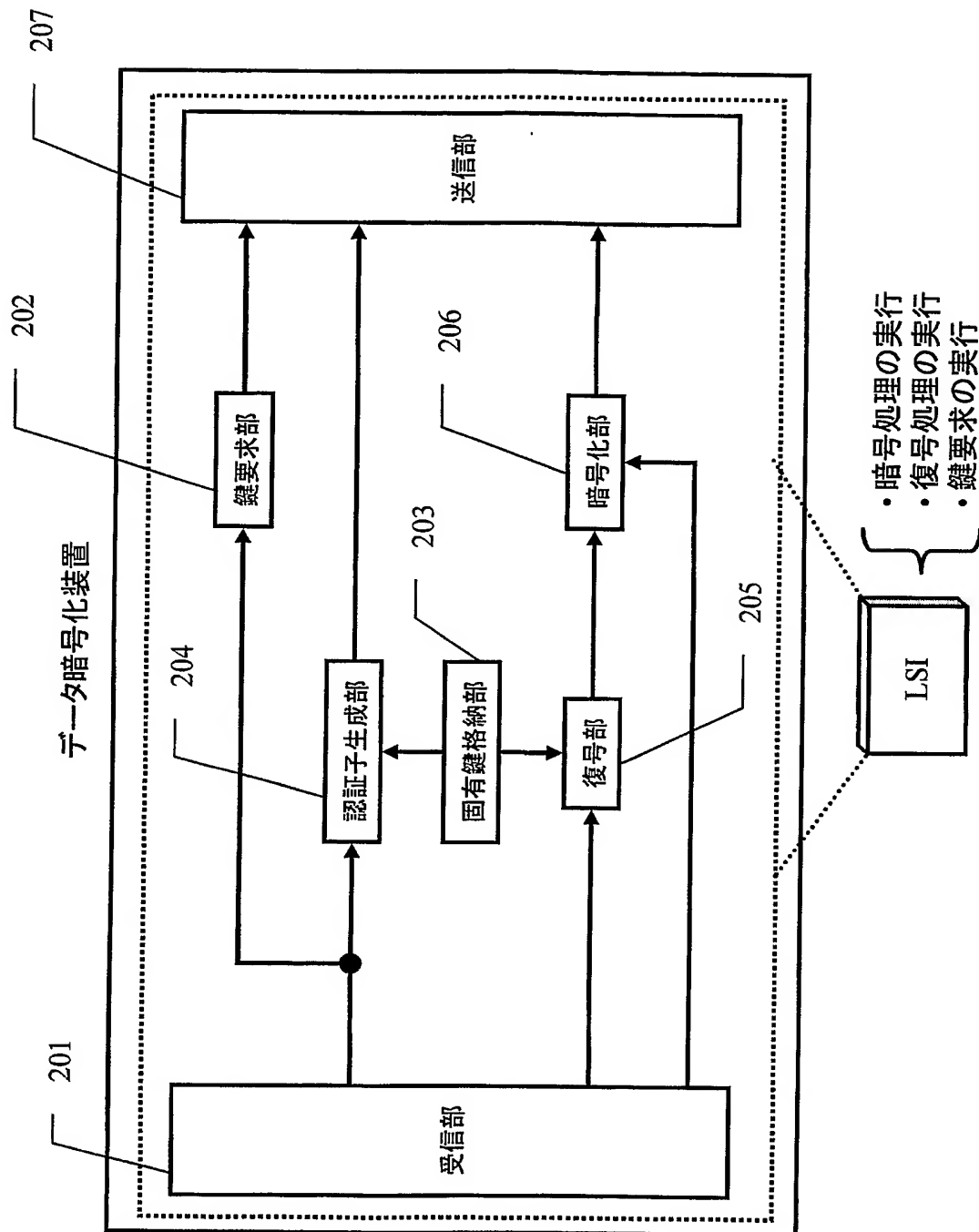
- 101 データ配布装置
- 102 データ暗号化装置
- 103 データ暗号化装置
- 104 鍵配布装置
- 201、501 受信部
- 202 鍵要求部
- 203 固有鍵格納部
- 204 認証子生成部
- 205 復号部
- 206、508 暗号化部
- 207、509 送信部
- 502 検証鍵格納部
- 503 署名検証部
- 504 データ暗号化装置固有鍵格納部
- 505 認証子検証部
- 506 鍵生成判定部
- 507 鍵生成部

【書類名】 図面

【図 1】




【図 2】



【図 3】

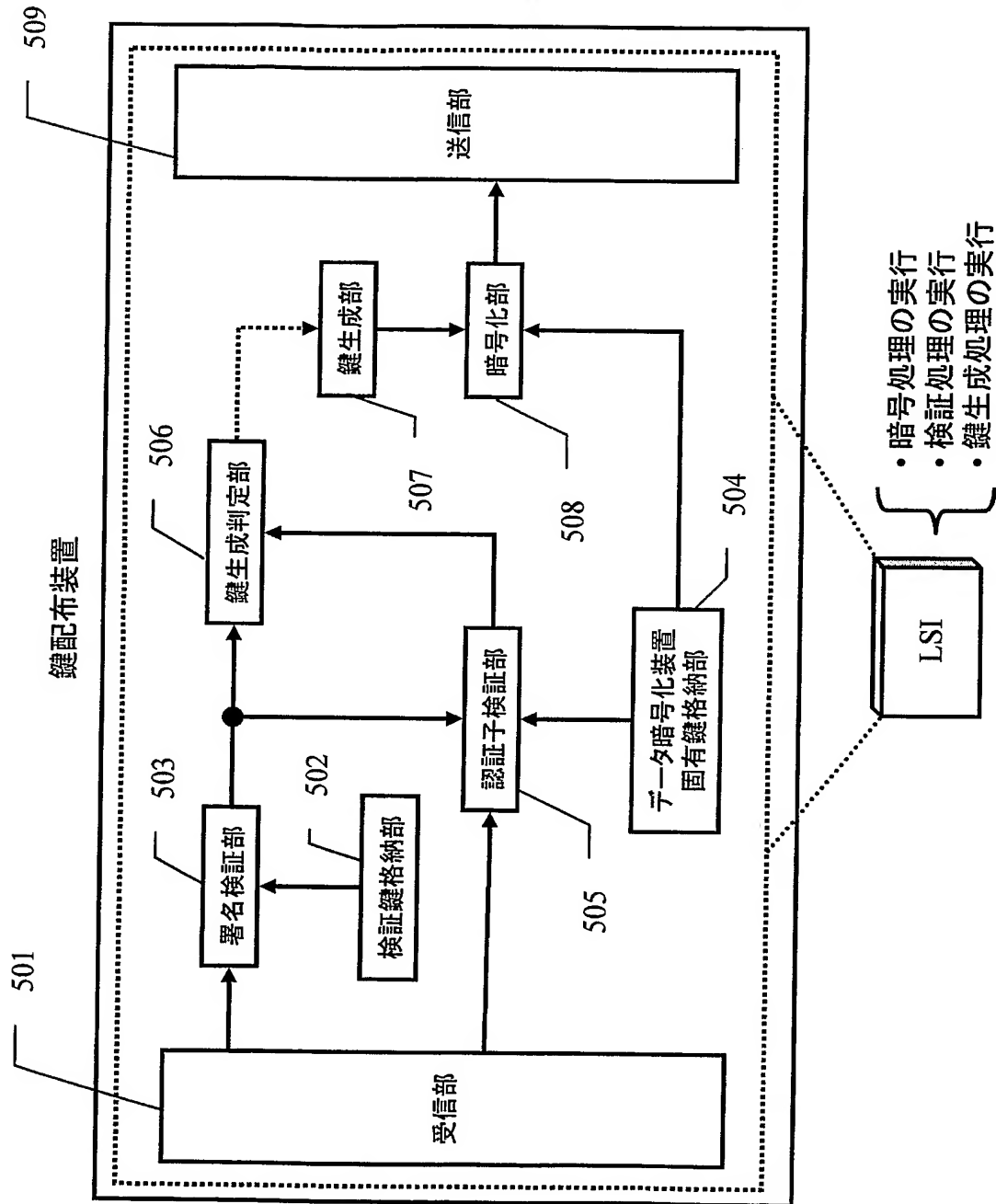
許可証の発行日 : DATE	20031104
暗号化を許可する装置 : ID1	0x000001
データ配布装置による署名 : SIG	Sig(SK_dd, DATE ID1)



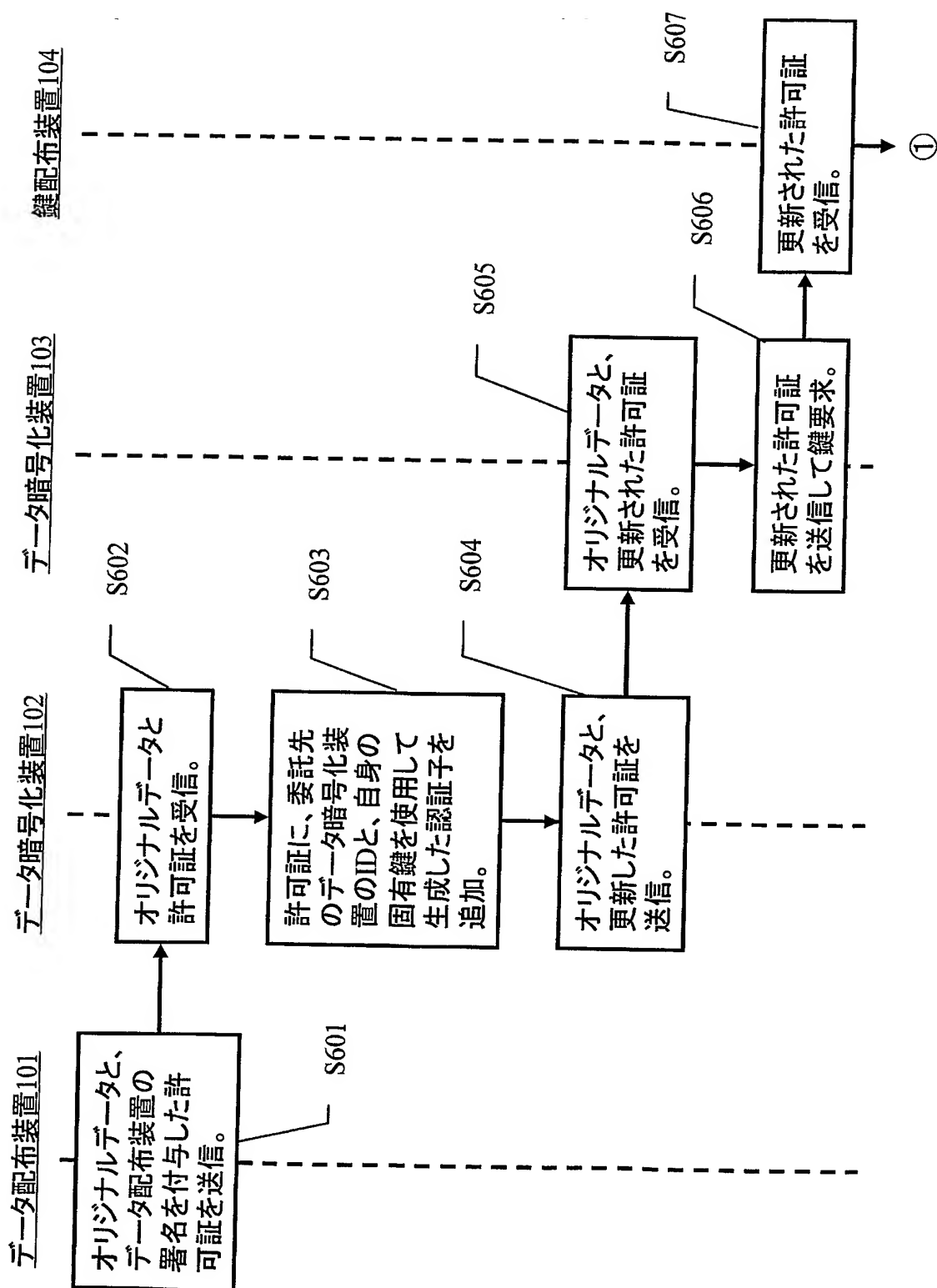
【図 4】

許可証の発行日 : DATE	20031104
許可するデータ暗号化装置 : ID1	0x000001
データ配布装置による署名 : SIG	Sig(SK_dd, DATE ID1)
暗号化を委託するデータ暗号化装置 : ID2	0x000002
データ暗号化装置1による認証子 : MAC	Mac(K1, DATE ID1 SIG ID2)

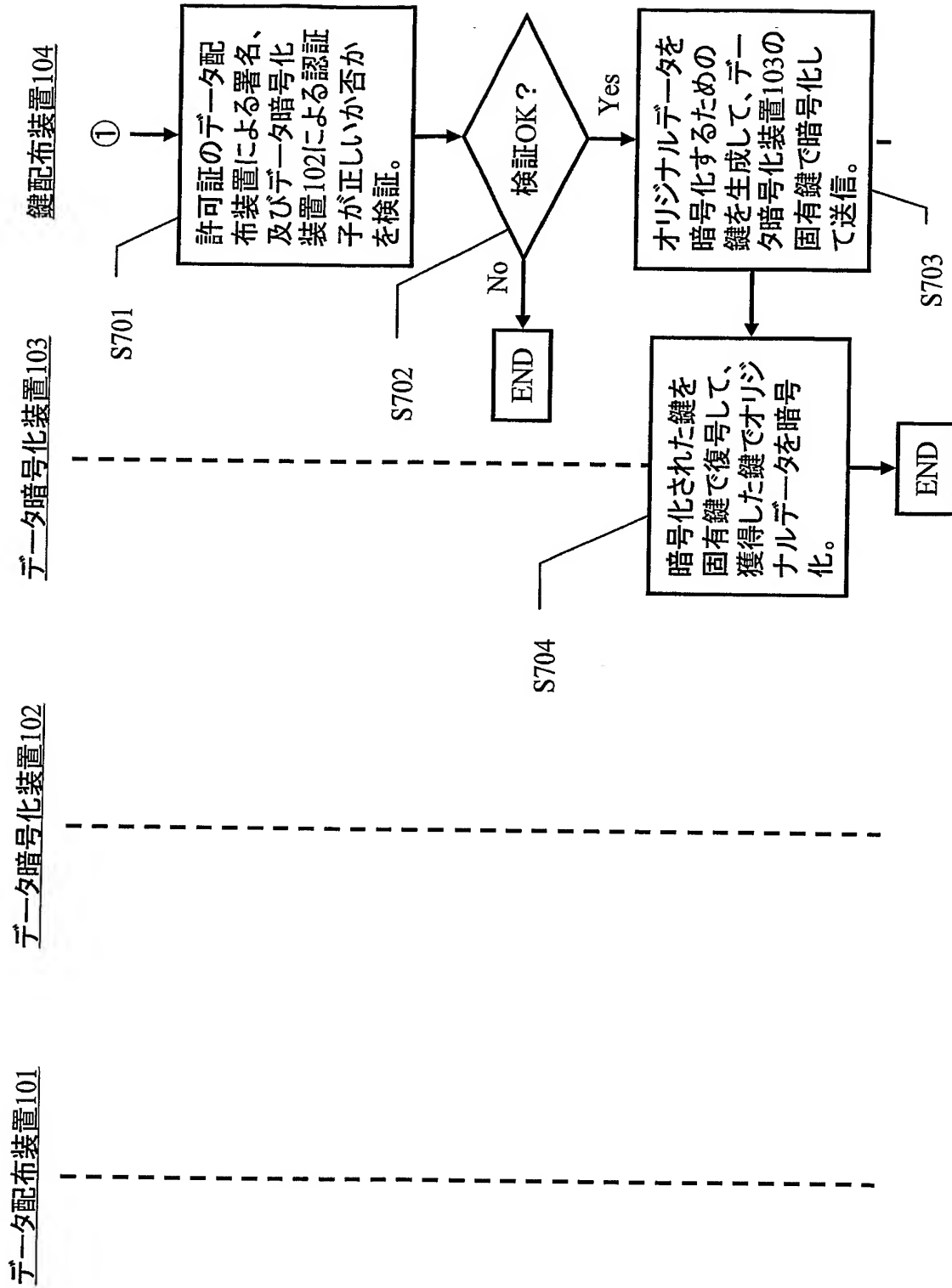
【図 5】



【図 6】



【図 7】



【書類名】 要約書**【要約】**

【課題】 許可証を受け取った装置だけが暗号化処理、あるいは復号処理を実行することが可能となるシステムでは、実際の処理を、正規に他の装置に対して依頼（委託）することが不可となってしまうシステムの柔軟性が損なわれる。

【解決手段】 著作権保護システムは、コンテンツデータを供給するデータ配布装置 1 0 1 と、コンテンツデータを獲得して暗号化を実行するデータ暗号化装置 1 0 2、及び 1 0 3 と、コンテンツデータを暗号化するための鍵を配布する鍵配布装置 1 0 4 からなる。当該データ暗号化装置だけが個別に保持する固有鍵に基づいて許可証を更新することにより、他の装置に対する正規の処理委託を可能にする。

【選択図】 図 1

特願 2 0 0 4 - 0 7 3 0 8 6

出 願 人 履 歴 情 報

識別番号

[0 0 0 0 0 5 8 2 1]

1. 変更年月日

1 9 9 0 年 8 月 2 8 日

[変更理由]

新規登録

住 所

大阪府門真市大字門真 1 0 0 6 番地

氏 名

松下電器産業株式会社